

Tidelift

*Managed open source for application development teams
created in partnership with open source maintainers*

TIDELIFT

Agenda

- **Introductions**
- **Recap of what we know about United States Geological Survey today.**
Members of USGS Team to acknowledge accuracy, add or clarify.
- **Tidelift Overview**
- **Open Discussion, Questions and Answers**
- **Technical Review**
- **Next Steps**

Tidelift Account Team

Matthew Arnow- Enterprise Account Executive
Brooklyn, New York

Melanie Gonglach- Account Executive
Boulder, Colorado

Jesse Houldsworth - Solutions Architect
Berkshires, Massachusetts

Josh Gallant - Business Development Representative
Boston, Massachusetts

What we've heard from the National Geospatial Technical Operations Center - U.S.G.S team to date:

- The NGTOC - USGS sits within the Department of Interior and in the process of transitioning completely to open source (Oracle Apex) which is a large two year effort
 - Also building with Django, Python, Postgress and many others
- Challenges with Dependencies Include:
 - Different versions
 - Open source compatibility (Spring Roo and certain versions of Maven, TomCat)
 - USGS has needed to *"find the sweet spot"*
 - Identifying and selecting what components to use, each teams have different needs
 - Ensure NGTOC is only working with known safe and secure components which are authorized by DOI.
- Scott has 5 engineers on his team and represents one of seven development teams that all role up to Derek Masaki.
- Scott would like to have Tidelift in use to help manage the open source components being used now and in the future within USGS.

Professional-grade open source software— managed for you. *What we like to call* **Managed Open Source**

Tools. The tools to keep track of all the dependencies you use, flag issues, and enforce policies.

Management. Management of core, mission-critical packages on your behalf, including researching and resolving issues so you don't have to anymore.

Maintainers. Recruiting maintainers for many important projects and paying them to proactively prevent problems and address the root causes of issues.

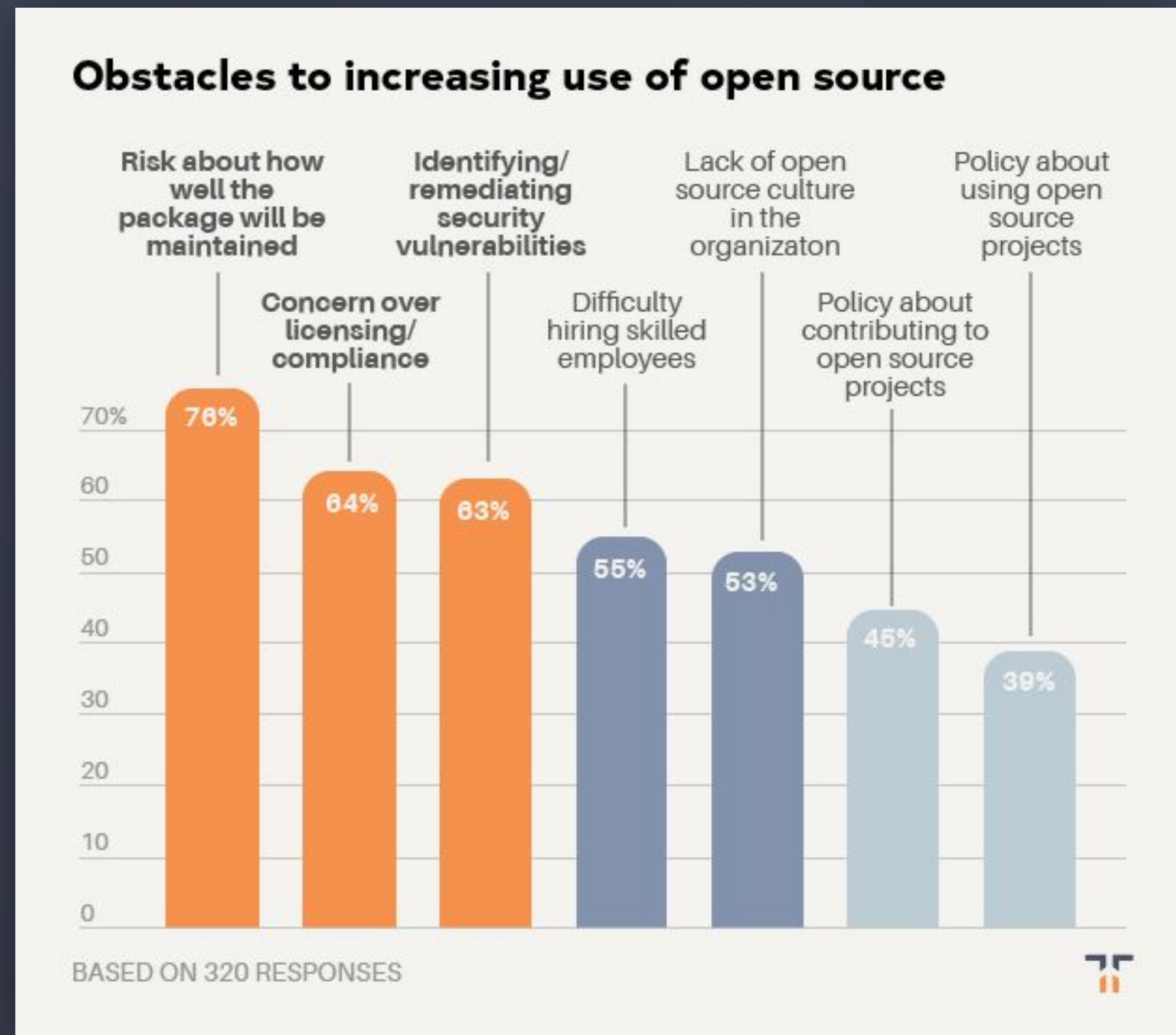
Tidelift, the *managed open source* subscription

- Enterprise-class open source subscription like Red Hat, MongoDB, HashiCorp or Elastic but covering JavaScript, Python, Ruby, PHP, Java, and .NET
- Helps development teams save time and reduce risk when using open source to build applications
- Thousands of packages directly supported by maintainers as part of the Tidelift Subscription, with new maintainers signing up every day
- Partnerships with Python Software Foundation, Ruby Together, NumFOCUS and more

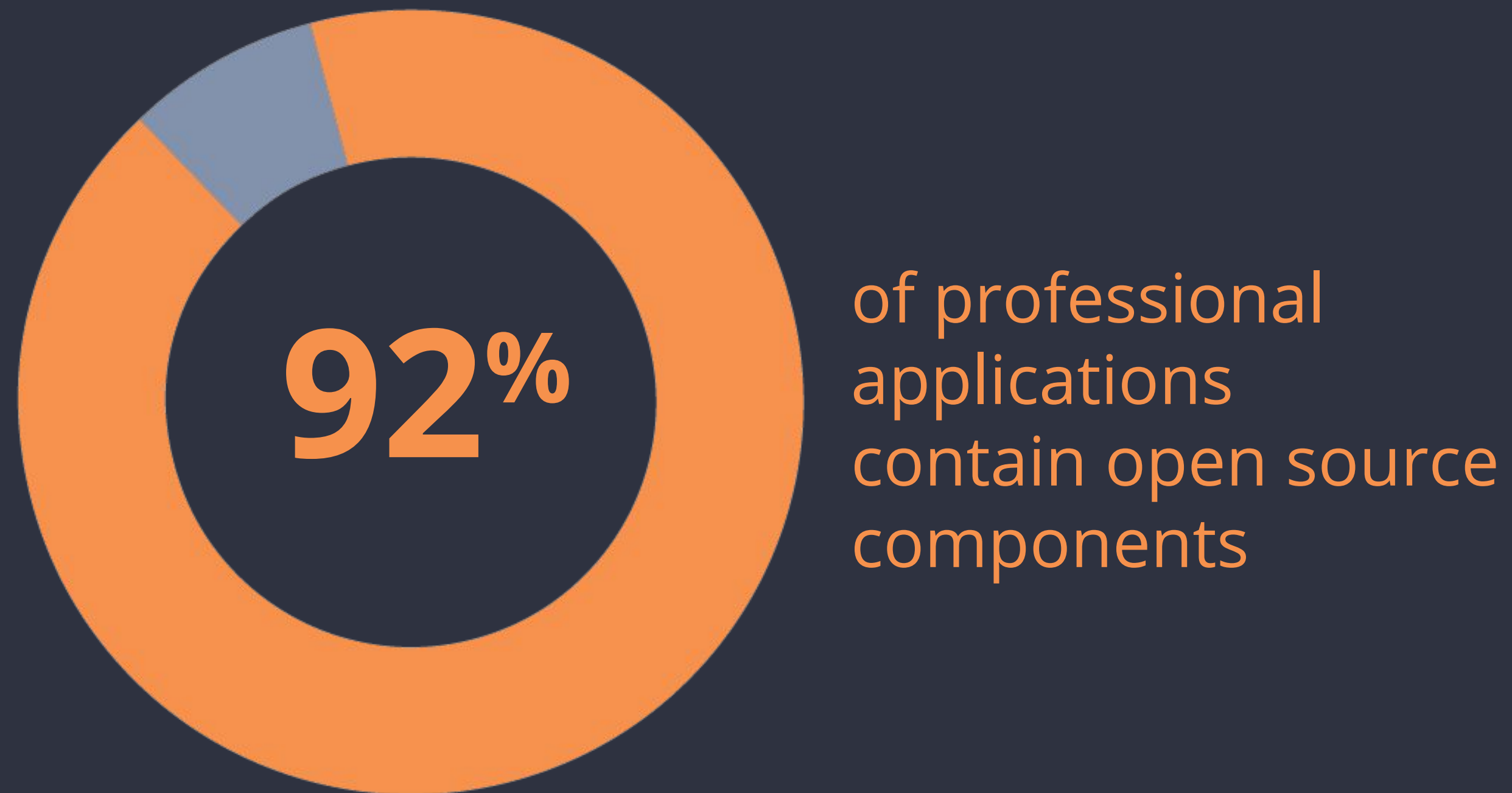
The big three support challenges: maintenance, security, and licensing

In multiple surveys, the biggest obstacles for development teams using open source have been remarkably consistent:

- Maintenance
- Security
- Licensing

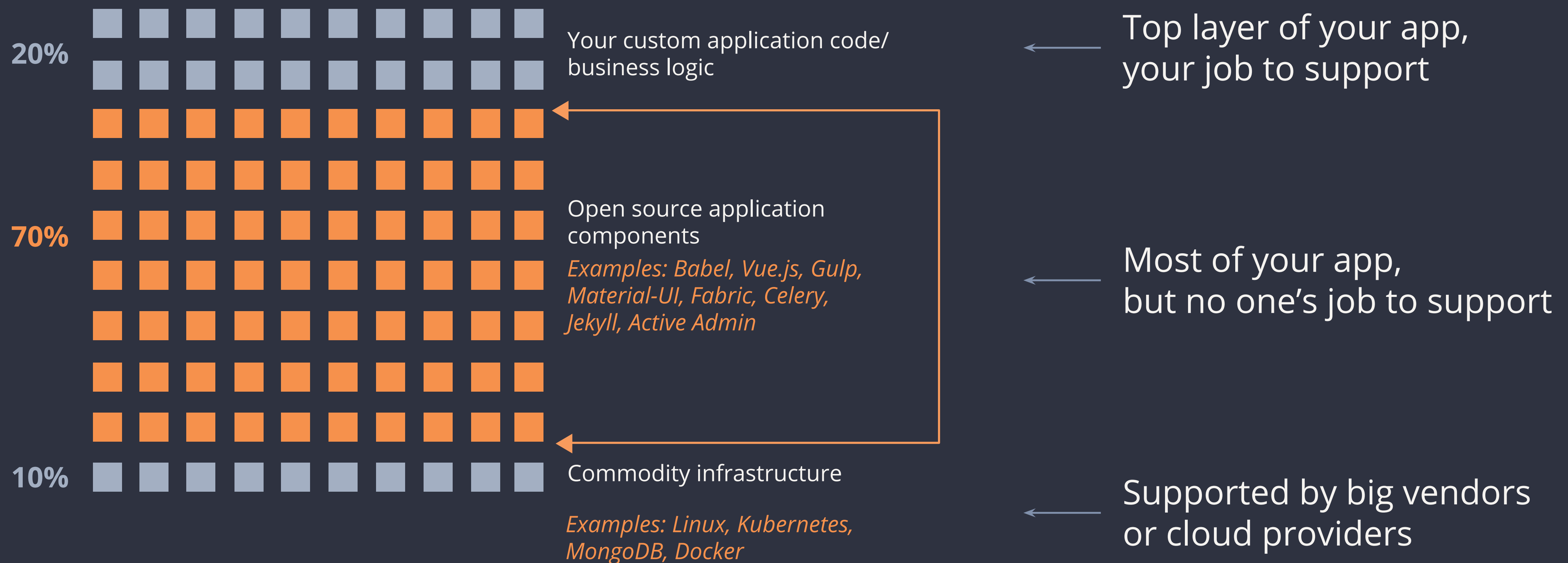


Open source = the modern development platform



- It is fundamental to the development process and essential for building applications
- It is a blessing (productivity boost) and a curse (dependency hell and other maintenance headaches)

Most applications are built on top of a foundation of 70% or more open source code



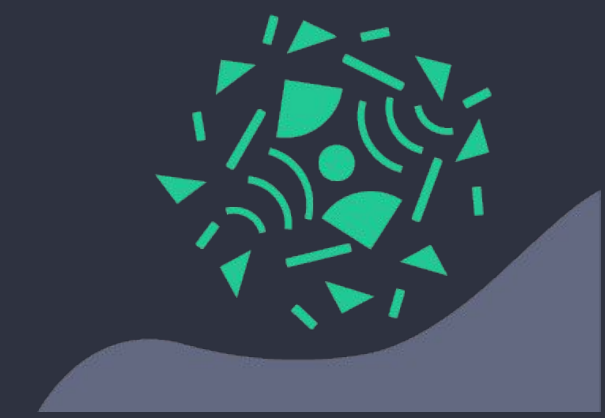
Key benefits of the Tidelifft Subscription



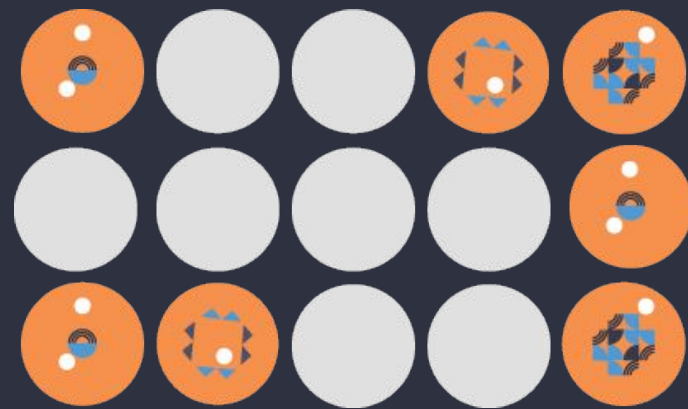
Security updates



Licensing verification and indemnification



Maintenance and code improvement



Package selection and version guidance

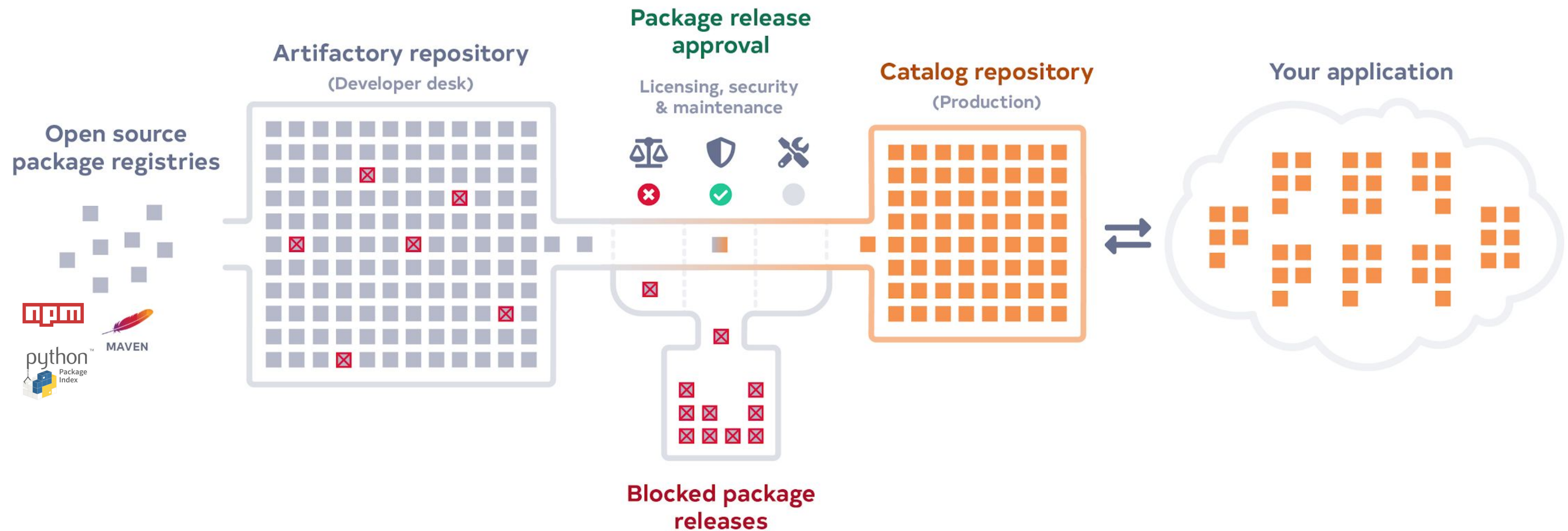


Roadmap input



Tooling and cloud integration

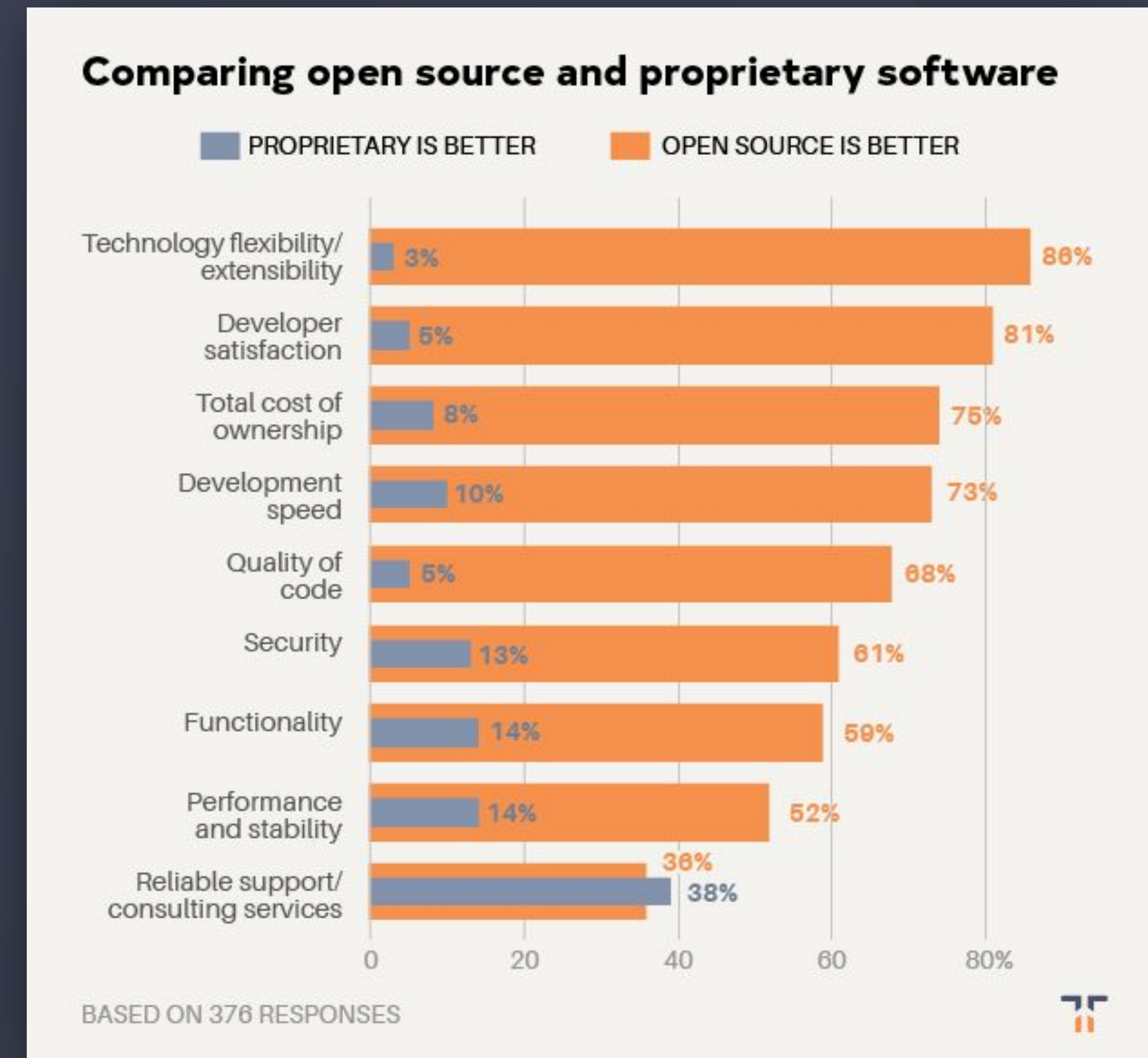
How packages move from upstream to production



Who's supporting the 70% of components you use to build your apps?

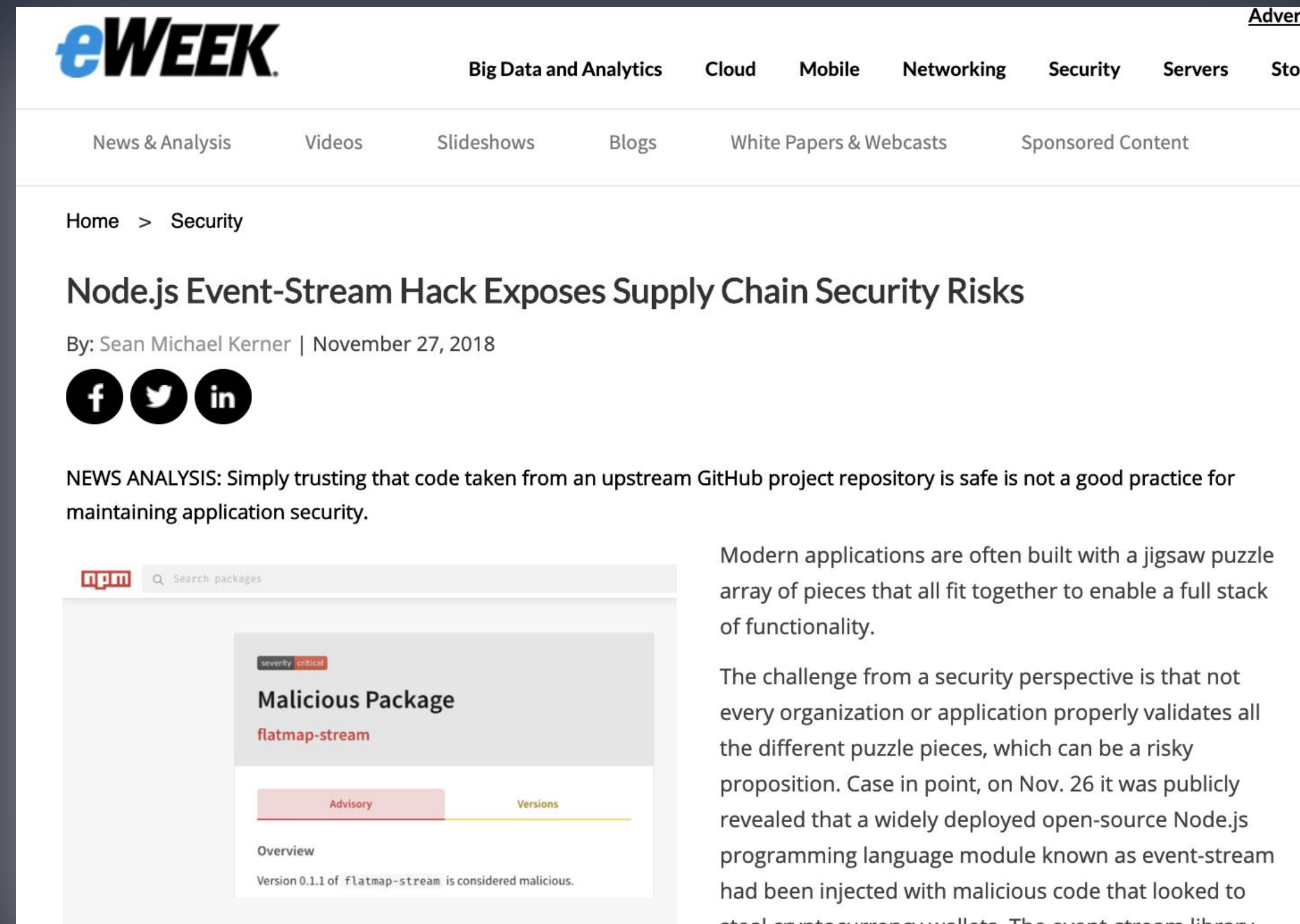
Historically, reliable support for open source is the only pain reported by many development teams.

Open source outclasses proprietary software in every other category.



What can happen when code isn't professionally maintained?

One example:
event-stream, an npm
package with over 100
million downloads and
no active maintainer, is
taken over by a malicious
actor trying
to steal bitcoin.



The screenshot shows the eWEEK website with a navigation bar including categories like Big Data and Analytics, Cloud, Mobile, Networking, Security, Servers, and Storage. Below the navigation bar, there's a breadcrumb trail: Home > Security. The main article title is "Node.js Event-Stream Hack Exposes Supply Chain Security Risks" by Sean Michael Kerner, dated November 27, 2018. Social media sharing icons for Facebook, Twitter, and LinkedIn are present. A "NEWS ANALYSIS" section states: "Simply trusting that code taken from an upstream GitHub project repository is safe is not a good practice for maintaining application security." Below this, there's a screenshot of the npm website showing a "Malicious Package" alert for "flatmap-stream". The alert indicates that "Version 0.1.1 of flatmap-stream is considered malicious." To the right of the npm screenshot, the article text begins: "Modern applications are often built with a jigsaw puzzle array of pieces that all fit together to enable a full stack of functionality. The challenge from a security perspective is that not every organization or application properly validates all the different puzzle pieces, which can be a risky proposition. Case in point, on Nov. 26 it was publicly revealed that a widely deployed open-source Node.js programming language module known as event-stream had been injected with malicious code that looked to steal cryptocurrency wallets. The event-stream library..."

Other horror
stories

EQUIFAX



heartbleed

A NEW APPROACH

Managed Open Source

A way for application development teams
to offload the complexity
of managing open source components.

Save time. Reduce risk.



The Tidelift Subscription

Managed open source for application development teams

The Tidelift Subscription is a managed open source subscription for application dependencies covering millions of community-led open source projects across JavaScript, Python, Java, PHP, Ruby, .NET, and more.

Save time. Reduce risk.





Security updates

Tidelift's security response team coordinates patches for new security vulnerabilities and alerts immediately through a private channel, to keep your software supply chain more secure.

design-system > scan #413

These issues are blocking your build.

lodash 4.17.11

(786KB; npm package in your manifests)

This package is potentially vulnerable to [CVE-2019-10744](#).

Consider switching from 4.17.11 to 4.17.15
[see all versions](#)

This is a direct dependency, so you can fix this yourself by upgrading this package.



Licensing indemnification and verification

Tidelift verifies license information to enable easy policy enforcement and adds intellectual property indemnification to cover creators and users in case something goes wrong.

dependencyci

We've researched these licenses so you can enforce your licenses policies with confidence.

> Converted to SPDX format (11)

> Lifter verified (13)

> Correct (251)

Licenses research

Needs Research

A package has no known license	unlicensed	fail
A release has security vulnerabilities	vulnerable	fail
A release has known critical bugs	broken	fail
A package uses a disallowed license	license_prohibited	fail
A package is using an inactive release stream	inactive_stream	warn



Maintenance and code improvement

Tidelift ensures the software you rely on keeps working as long as you need it to work. Your managed dependencies are actively maintained and we recruit additional maintainers where required.

bibliothecary tasks

OPEN TASKS COMPLETED TASKS

September 16th, 2019

Two-Factor Authentication was confirmed as enabled.

September 3rd, 2019

Release Streams verified by katzj.

August 9th, 2019

Broken version notification for 1.3.0 by tiegz.

July 29th, 2019

Broken version notification for 0.2.0 by kbarrette.

Release Streams verified by kbarrette.

July 25th, 2019

Release notes entered or verified.

June 25th, 2019

Two-Factor Authentication was confirmed as enabled by tiegz.

June 11th, 2019

Package dependencies scan fixed with version 6.8.5.

Create a Coordinated Disclosure Plan

Let us know how you'll handle security reports.

START TASK

Setup Two-Factor Authentication

Secure your packages with Two-Factor Authentication.

START TASK

Add Release Notes

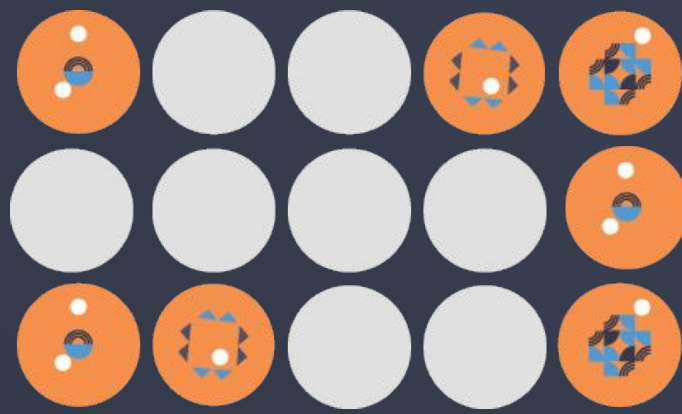
Add release notes to package releases.

START TASK

Release Streams

We will ask you what versions of this package are active, stable, deprecated, or broken.

START TASK



Package selection and version guidance

We help you choose the best open source packages from the start—and then guide you through updates to stay on the best releases as new issues arise.

nokogiri (rubygems) LIFTED

Nokogiri (鋸) is an HTML, XML, SAX, and Reader parser. Among Nokogiri's many features is the ability to search documents via XPath or CSS3 selectors.
Latest stable release: 1.10.5

[TALK TO THE MAINTAINERS](#)

OVERVIEW

- ✓ Verified MIT license
- ✓ Recent commit activity
- ✓ Coordinated disclosure policy [↗](#)

COMMUNITY

- ✓ Recent issues and pull requests being or closed
- 166 contributors

[nokogiri](#)

nokogiri version guidance LIFTED

1.10.* is the current recommended release stream

1.10.5 is the current recommended version on 1.10.*, and is also the latest version

1.10.0.rc1, 1.10.0, 1.10.1, 1.10.2, 1.10.3, 1.10.4, and 1.10.5 have no problems

1.9.* is inactive and will no longer receive security updates

1.9.0, 1.9.0.rc1, and 1.9.1 have no problems

1.8.* is inactive and will no longer receive security updates

1.8.0, 1.8.1, 1.8.2, 1.8.3, 1.8.4, and 1.8.5 have no problems

1.7.* is inactive and will no longer receive security updates

1.7.0, 1.7.0.1, 1.7.1, and 1.7.2 have no problems

1.6.* is inactive and will no longer receive security updates

1.6.0, 1.6.1, 1.6.2, 1.6.2.1, 1.6.2.rc1, 1.6.2.rc2, 1.6.2.rc3, 1.6.3, 1.6.3.1, 1.6.3.rc1, 1.6.3.rc2, 1.6.3.rc3, 1.6.4, 1.6.5, 1.6.6.1, 1.6.6.2, 1.6.6.3, 1.6.6.4, 1.6.7, 1.6.7.1, 1.6.7.2, 1.6.7.rc2, 1.6.7.rc3, 1.6.7.rc4, 1.6.8, 1.6.8.1, 1.6.8.rc1, 1.6.8.rc2, 1.6.8.rc3, and 1.6.4.1 are vulnerable to [CVE-2013-6461](#) [↗](#)

1.6.0.rc1 has no problems

1.10.1 8%

recommended receives updates prerelease has issues

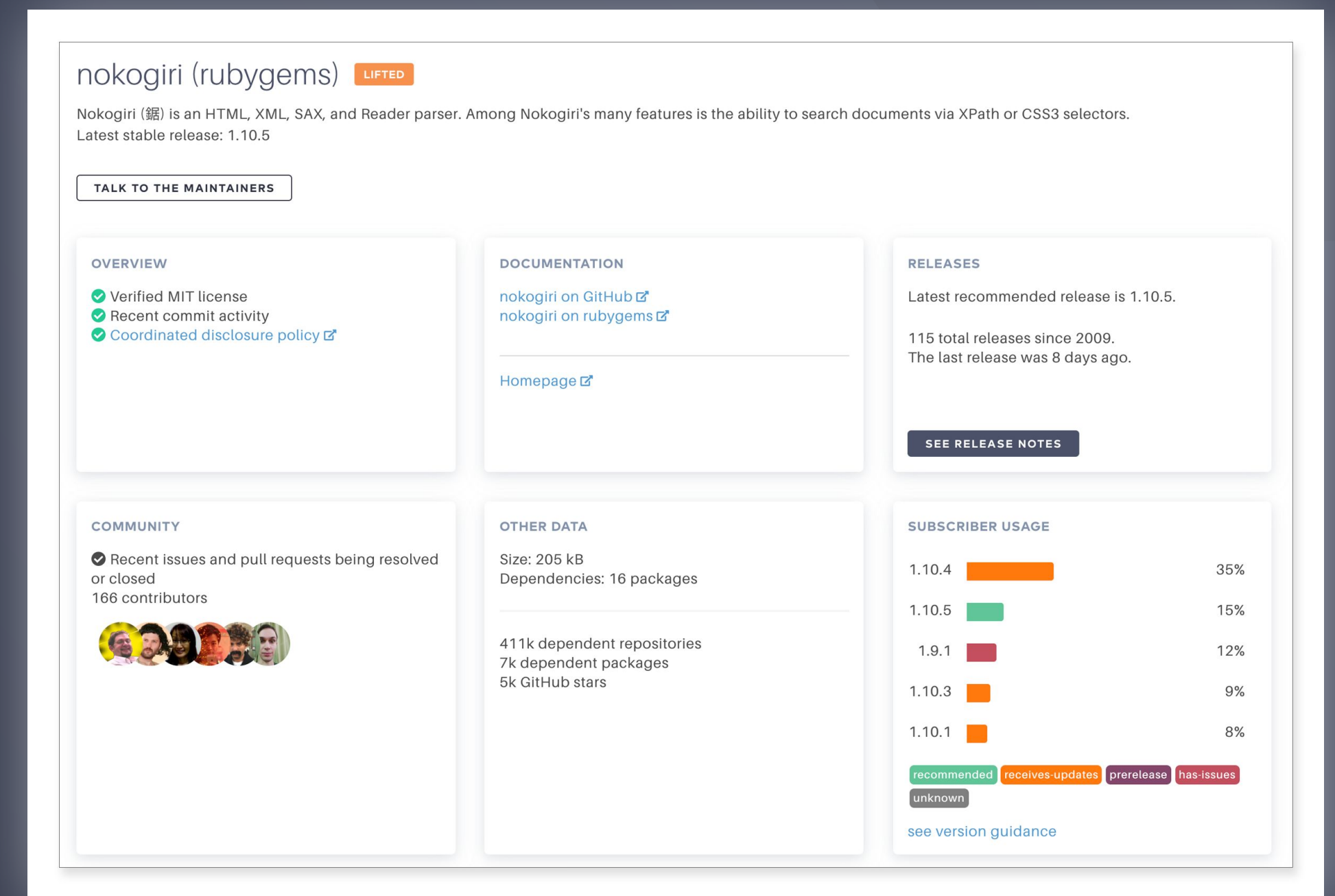
unknown

[see version guidance](#)



Roadmap input

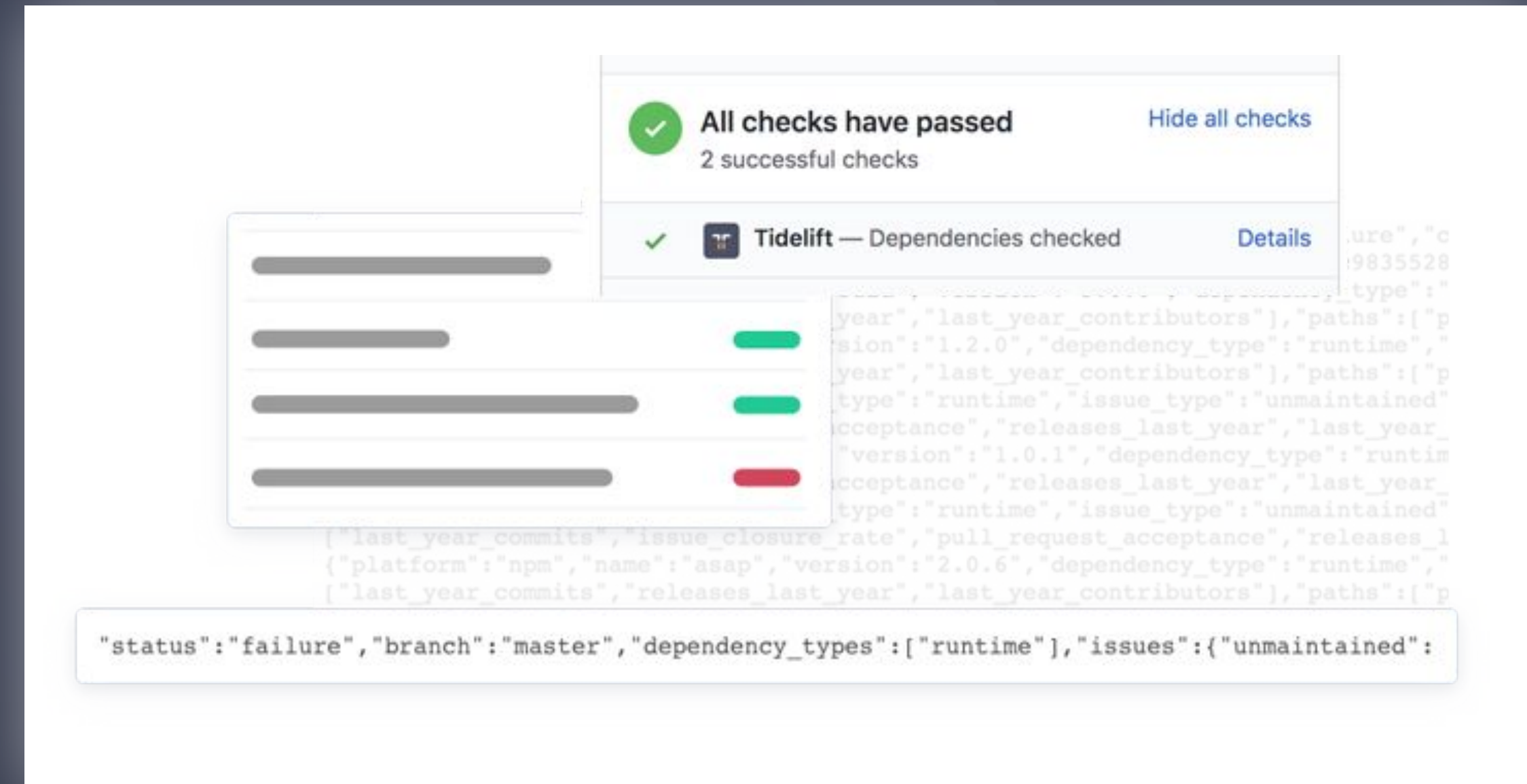
Take a seat at the table with the creators behind the software you use. Tidelift's participating maintainers earn more income as their software is used by more subscribers, so they're interested in knowing what you need.





Tooling and cloud integration

Tidelift works with GitHub, GitLab, Bitbucket, and more. We support every cloud platform (and other deployment targets, too).



Bottom line:

All the capabilities you expect and require from commercial software.

But now, for all of the key community-led open source software you depend on.



Thank you